ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 9, No. 4, December 2021, pp.1070-1082

Adopt an optimal location using a genetic algorithm for audio steganography

Alaa Q. Raheema
Civil Engineering Department, University of Technology-Iraq, 10001 Baghdad, Iraq

ABSTRACT

With the development of technologies, most of the users utilizing the Internet for transmitting information from one place to another place. The transmitted data may be affected because of the intermediate user. Therefore, the steganography approach is applied for managing the secret information. Here audio steganography is utilized to maintain the secret information by hiding the image into the audio files. In this work, discrete cosine transforms, and discrete wavelet transform is applied to perform the Steganalysis process. The optimal hiding location has been identified by using the optimization technique called a genetic algorithm. The method utilizes the selection, crossover and mutation operators for selecting the best location. The chosen locations are difficult to predict by unauthorized users because the embedded location is varied from information to information. Then the efficiency of the system ensures the high PSNR, structural similarity index (SSIM), minimum mean square error value and Jaccard, which is evaluated on the audio Steganalysis dataset.

Keywords: steganography; genetic algorithm; selection, mutation; cross over; structural similarity Index; and audio Steganalysis dataset.

Corresponding Author:

Alaa Q. Raheema
Civil Engineering Department
University of Technology-Iraq
Baghdad, Iraq.
40345@uotechnology.edu.iq

1. Introduction

The development of technologies and internet usage creates a significant impact on a human day to day lifestyle [1, 2]. The involvement of the technical process requires an enormous amount of information for processing the request that depends on user requirements [3]. This process requires continuous information transmission; here, the security of the information placed a vital role. There are several cryptography and steganography technologies [4-6] are utilized to maintain data security. Compared to the encryption techniques, steganography manages the quality and safety of data. Primarily, the audio steganography provides a way to hide the transmitting information into the audio signal and create the Stego key that minimizes the unauthorized activities on the information [7-9]. Audio steganography is a challenging because it entirely depends on the Human Auditory System (HAS) [10], which frequency range varied dynamically. Therefore, effective methodologies should be introduced to processing the audio signal for embedding and extracting the text in both the sender and receiver sides. The created steganography methods must be maintaining the robustness and information security characteristics for denying unauthorized access [11-13]. This audio steganography process is utilized in several applications such as bank transactions, battlefield communication, etc. By embedding the secrete messages into the audio files, the audio file's binary representation slightly changed. The changes in the binary audio sequence create more complexity while accessing the data file during information transmission. With the consideration of audio characteristics and the human auditory system (HAS), several methods [14-17] such as least significant bit (LSB) coding, parity coding, phase coding, and spread spectrum coding techniques are developed to perform the audio steganography process [18-20]. These methods are few pitfalls such as non-provision of the encryption key, limited secret message length up to 500, absence of frequency chart variations, time is taken to perform the decode and encoding process, and user interface lack. These difficulties are continuously affecting the entire audio steganography process. For overwhelming this issue, in this work, a discrete wavelet transform (DCT)

and discrete cosine transform (DCT) were utilized to examine the audio steganography process [21-23]. The hybrid method of DWT and DCT approach manages the audio parameters like strength, clearness temper resistance, undetectability, robustness, invisibility and capability. These audio signal parameters help to hide the secrete messages in the carrier and establish the secure communications system; also recognize the Steganalysis attacks successfully [24-26]. The hybrid DWT and DCT approach analyze the input audio signal and images for extracting the approximation and detailed coefficients. These coefficients are more helpful to hide the secrete messages into the audio signal. Here, the genetic algorithm is utilized to embed the secret messages into the audio file to deny intermediate access. The genetic algorithm uses different operators such as selection, crossover and mutations. These operators examine the audio frequencies and respective frames to predict the embedding location successfully. Due to this reason, in this work, a hybrid DWT and DCT technique with a genetic algorithm is applied to perform the audio steganography process. The created steganography process manages the data quality, security and able to resolve the pitfalls of the traditional method. The introduced audio steganography process is developed using MATLAB tool and the excellence of the system is evaluated using the Audio Steganalysis dataset. The remaining structure of the manuscript is formulated as section 2 analyzes the various researcher's opinions on the audio steganography process. Section 3 examines the optimal location using a genetic algorithm for audio steganography, and the system's efficiency evaluated in section 4. Conclusion discussed in section 5.

2. Related works

Taouil Y. et al., developing the image steganography process by applying the Haar discrete wavelet transform [27]. This process is used to hide the data in the frequency domain because of the robust area. The embedding process is achieved in the integer part that helps to avoid data loss also improves the high imperceptibility and image quality. The data is embedded in the image according to the random essential selection, which selects the data hiding location randomly. Tanwar R. et al., optimizing the audio steganography using opinion formation [28]. This process utilizes the human opinion formulation process for resolving the computational problems. By integrating the human opinion and steganography process, the data quality is further improved along with security. Zhang Z. et al., applying deep residual networks for maximizing the performance of audio Steganalysis in the temporal domain [29]. Initially, the residual map had estimated for the audio signal to determine the difference between the Stego and cover. Then, convolution neural networks are applied to identify the steganography complex statistical features. After extracting the features, normalization layers are applied to predict the connection between the components, which helps perform the Steganalysis. During this process, over-fitting issues are resolved by using the back-propagation learning process. Biswas, R. et al., performing the color image steganography process by applying the genetically optimized 2D- discrete cosine transform [30]. This system can work against the brutal attack and rigorous testing due to the successful embedding process into the images. Here, the genetic algorithm improves the overall robustness of image steganography and the embedding location is selected randomly. This process improves the overall data security and the implemented using StirMark 4.0 benchmark tool. The created system ensures effective results such as receiver operating curve (ROC) values on steganography analysis. Alwahbani S.M.H. et al., performing the audio steganography and cryptography process by applying the least significant bit with a one-time pad approach [31]. This process uses the two chaotic maps such as logistic and piecewise linear chaotic maps to perform the encryption process. Then the encrypted messages are hidden in the audio by generating a chaotic sequence. The encrypted information is embedded into the audio according to the least significant bit. This process ensures the steganography robustness, data hiding capacity and perceptual transparency characteristics. A. H. Mohsin et al., developing the steganography process in the spatial domain according to the particle swarm optimization [32]. Here, the secrete message related bits are analyzed and modified, which are embedded in the host image. During the embedding process, the data hiding location is identified according to the particle swarm optimization process. From the located region, the least significant bit (LSB) based information has to hide. This process efficiency is evaluated using benchmark analysis, in which the system ensures 45.13% of the PSNR value. Luo W. et al., creating the audio steganography by applying the advanced audio coding with the syndrome trellis coding [33]. Initially, the audio file is compressed using an advanced audio coding process and the residual signal value is compared with before and after compression. Finally, syndrome-trellis coding was applied to perform the embedding process and created the Stego audio. The effectiveness of the system evaluated using 10,000 speech audio clips and 10,000 music in which coding based audio steganography ensures effective results. Dalal M., et al., surveying the video steganography techniques presented in the spatial domain

[34]. This process examines the various spatial domain steganography techniques to manage steganography parameters such as robustness, imperceptibility, and capacity. More ever, this process is used to resolve the statistical complexity and extensive size data handling issues. According to the various researcher's opinions, audio steganography is a crucial process to manage data security and quality. Although these discussed techniques are achieving better results, the audio steganography's effectiveness should be increased due to the complexity and challenging task. Here, the discrete wavelet transform and discrete cosine transform approaches are applied to the audio signal and image message. During the embedding process, a genetic algorithm is applied to select the embedding location of confidential data. The optimization algorithm uses different operators to manage the security of the data from unauthorized activities. The detailed working process of the audio steganography process is explained in the subsequent section.

3. Optimization algorithm-based audio steganography process

The hybrid discrete wavelet transform (DWT) and discrete cosine transform (DCT) with genetic optimization-based audio steganography process are discussed in this section. Here, the image messages are hidden into the audio file to improve the overall data quality and security. This process utilizes the genetic algorithm with respective operators to avoid the intermediate attack's involvement in the system. The steganography process is performed on both the sender and receiver sides, ensuring the authentication and authorization of the data. The detailed working process of sender-side audio steganography analysis is demonstrated in figure 1.

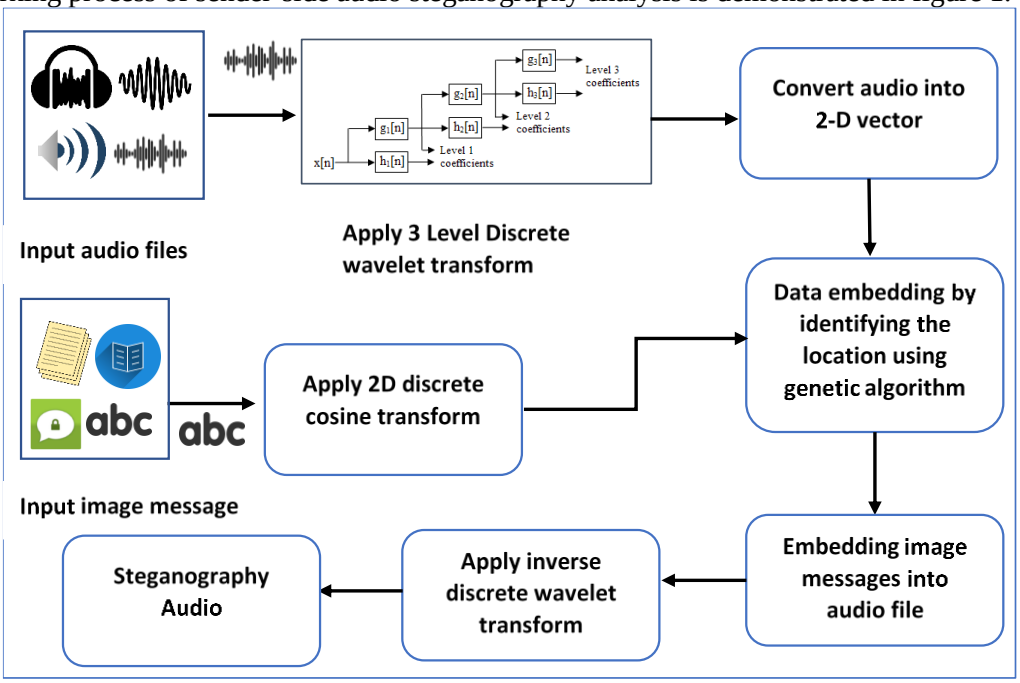

Figure 1. Image message with audio steganography analysis structure in the sender side

Figure 1 demonstrated the working process of image messages with the audio steganography process on the sender side. Here, a discrete wavelet transform process is applied to the audio file that generates the 2D vectors by computing the approximation and detailed coefficient. Then, discrete cosine transformation is applied to the image-based messages that create the embedding information. Finally, the genetic algorithm is utilized to identify the embedding location that is varied according to the genetic operators. Therefore, the optimized hiding location improves the overall data security, quality and eliminates unnecessary attacks in the system.

3.1. Steganography process in the sender side

The information is communicated from sender to receiver; here, several intermediate access and attacks eliminate the security and quality of data. Therefore, transmitting audio signals need to be altered in terms of binary sequence to avoid medium access and attacks. Hence, image messages are hiding in the audio signal to ensure the steganography requirements such as robustness, perceptual transparency and capacity. To achieve the main objective of this system, discrete wavelet transformation (DWT) is applied to decompose the original audio signal to different sub-signals by examining the approximation and detailed coefficients. Then the image

messages are further analyzed using cosine transform to get the hiding details. Additionally, the data hiding process improved by selecting the best and optimized hiding location by using a genetic algorithm. The discrete wavelet transform (DWT) is applied to the input audio signal because it is developed according to the short-time Fourier transform (STFT). The created 3-dimensional wavelet transform able to overcome the frequency and time domain resolution issue. The wavelet transform examines the input signal in each frame for obtaining the high-time and low-frequency resolution and low-time and high-frequency resolution details. As discussed earlier, the audio signals depending on the Human auditory system because the frequency and time resolutions are varied from one person to another. Therefore, the DWT approach is applied to the input signal to get the detailed and approximation coefficients and the DWT is derived from using eqn (1).

$$W(j,k) = \sum_j \sum_k x(k) 2^{-j/2} \psi\left(2^{-j} n - k\right) \quad (1)$$

The mother wavelet of the audio signal is computed with finite energy and fast decay from $W(j,k)$ represented in eqn (1). After identifying the mother wavelets, the series of high and low pass filters are applied to the input signal $\mathfrak{X}(n)$ to get the detailed and approximation coefficients. First, the input signal $\mathfrak{X}(n)$ is transmitted via the low pass filter with impulse response g; in the low pass filter, the convolution operation is performed to get the wavelet of input signal $\mathfrak{X}(n)$. The convolution process is achieved by applying eqn (2).

$$y(n) = (\mathfrak{X} * g)n = \sum_{k=-\infty}^{\infty} \mathfrak{X}(k) g(n-k) \quad (2)$$

High pass filter (h) is applied to the input signal $\mathfrak{X}(n)$ and decomposition is performed to get the detailed coefficients. The high and low pass filters produce the detailed and approximation coefficients of $\mathfrak{X}(n)$, which decompose the signal into sub-signals. The representation of three-dimensional discrete wavelet transform is illustrated in figure 2.

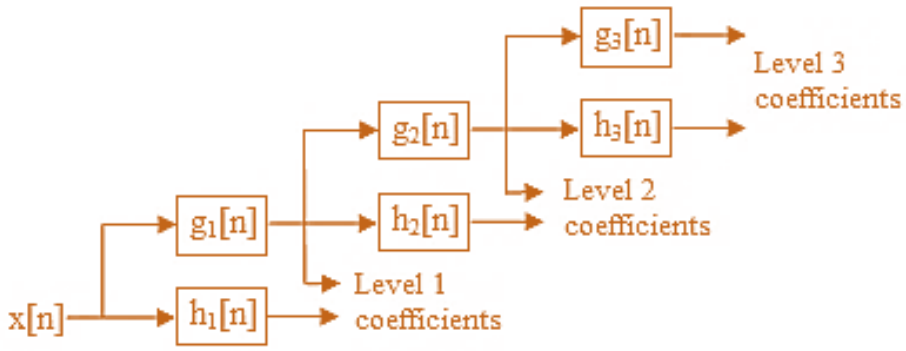

Figure 2. 3- Level discrete wavelet transform representation

After performing the audio signal decomposition process, the hiding secret image messages need to be analyzed using discrete cosine transform (DCT). The DCT method successfully works on images due to the various magnitudes and frequencies. In addition to this, the DCT method examines the spatial image information and minimizes the space occupancy which is done without affecting the image quality. This process computes the image spectral sub-bands respected to image visual quality and divide the images into low, high and middle frequencies. The method analyzes the images according to the DCT coefficient information and separates the images into the 8-by-8 blocks or 16-by-16 blocks. The divided blocks are examined separately to predict the discrete cosine transform values. Then the image decomposition is performed based on the two-dimensional discrete cosine transform process derived from a one-dimensional approach. The 2D-DCT formulation is performed using eqn (3).

$$X_{k_1,k_2} = \sum_{n_1=0}^{N_1-1} \left(\sum_{n_2=0}^{N_2-1} x_{n_1,n_2} \cos\left[\frac{\pi}{N_2}\left(n_2 + \frac{1}{2}\right) k_2\right]\right) \cos\left[\frac{\pi}{N_1}\left(n_1 + \frac{1}{2}\right) k_1\right] \quad (3)$$

Then the inverse 2D-DCT is performed by separable product of one dimensional at a time in the row-column process. The divided image sub spectral details are embedded into the audio signal to get the Stego audio to improve the overall data security. Here, the genetic algorithm is utilized to select the exact embedding location that maximizes the overall safety, authentication and maintains the steganography robustness. Then, the message present in the images are encrypted using advanced standard encryption approach. This process utilizes the different key values like 125, 192 and 256 bits to performing the encryption. The text encryption process is done by using eqn (4).

$$E(K,M) = (c)k \quad (4)$$

The cipher text $(c)k$ is obtained by applying the encryption function E on plain text M with respective encryption key K. After encrypting the messages in the image, it has to be embedded in the audio signal. Here, the least significant bit (LSB) utilized to perform the embedding process. At the time, higher position having the chromosome information that used to determine the optimal location for embedding the message into the audio. The optimal selection of embedding location increases the overall robustness of the system. From the collection of chromosomes, next generation chromosomes are selected based on the genetic operators such as selection, crossover and mutation. These operators are used to find the best chromosomes based on the fitness values which is chosen from the least significant bit layer position. This process used to get the new chromosome based on audio signal minimum deviation. Generally, the secret messages are embedded into the different layers of audio samples and get the new Stego sample. The position of the samples is varied but here genetic algorithm is utilized to select the best position for improving the overall steganography process robustness. More ever, this process minimizes the errors while embedding the data into the audio and never changes the audio quality that leads to maintains the capacity.

3.2. Embedding location detection using genetic algorithm

As discussed earlier, genetic algorithm utilized to identify the secret message embedding location; here the parameters are denoted as encoded binary string that is commonly called as chromosome. The chromosome having the elements which are denoted as gene; used to maximize and minimize the fitness value. During this process, genetic operators utilized to optimized the chromosome multiple variables for geniting the chromosome fitness value using fitness function. The genetic algorithm has several steps such as alteration, modification, verification and reconstruction to select the optimal embedding location.

3.3. Alteration

The first step of genetic algorithm based optimal embedding location identification is alteration. The alteration process analyzes the current generation solutions and select the good solution which is transmitted to the next candidate solution identification process. This process, target bits are utilized to replace the message bits which is done by simple substitution process.

3.4. Modification

The modification step plays a crucial role while selecting the secret message embedding location. This process used to reduce the error rate and maximize the transparency. The transparency is nothing but process of evaluating the audio signal distortion while embedding the messages into the audio. The transparency process does not affect the quality and content of audio signal but it was differing from original and Stego audio signal. In the first generation of genetic algorithm consists of original samples and modified samples, the fitness function is utilized on these samples for determining the error value. The fitness value is selected according to the most transparent patterns which are considered while performing the crossover and mutation process. In the crossover process, two individuals are mixed together and creating the next generation chromosome. The crossover process is named as the recombination because it rearranges only from existing chromosome characteristics. Then mutation operator is applied to the chromosomes in which random adjustments are performed.

3.5. Verification

After performing the modification step, quality controller step called verification is performed. Here, the mutation based generated outcomes are verified, the computed new samples are compared with the original samples. If the comparison is made, then the it is acceptable otherwise the mutation process is performed once again to predict the embedding location.

3.6. Reconstruction

After identifying the location from the genetic operator-based fitness function, the audio file is generated. Here, the secret message is embedded into the altered audio files. Then the working procedure of genetic algorithm illustrated in figure 3.

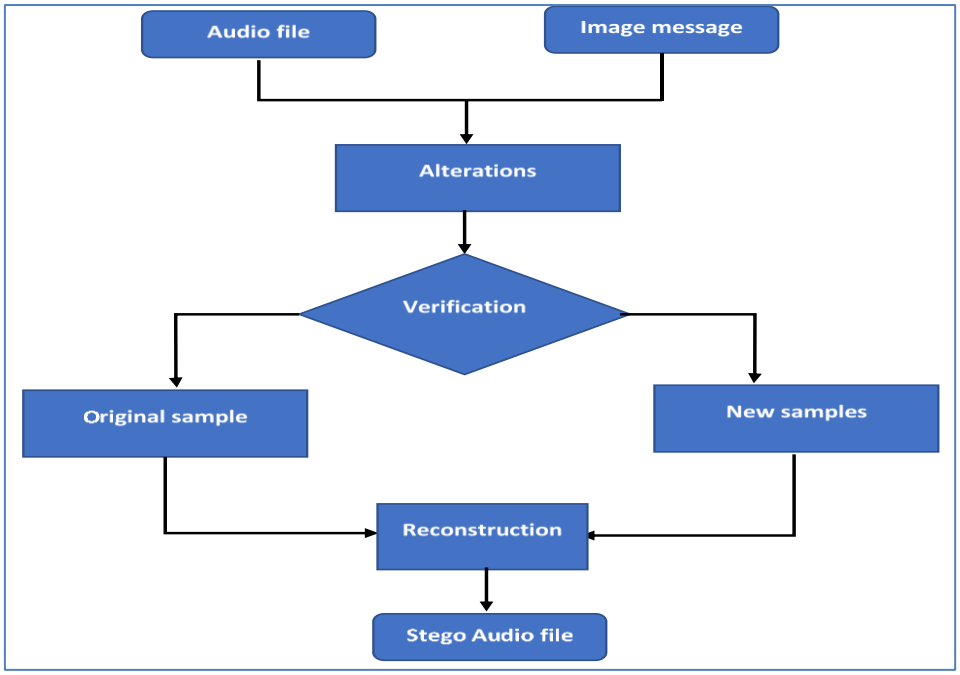

Figure 3. Genetic algorithm process for message embedding in audio file

Based on the above figure 2, the genetic algorithm selects the optimal embedding location in audio file. The selected locations are changed one audio from other audio. This process is repeated to get the Stego audio files. After that, the audio file is broadcast from sender to receiver side. In the receiver side, the Stego files frequency is examined using the inverse wavelet transform. The method retrieves the detailed and approximation coefficients from audio file. Afterwards, inverse DCT method is applied to get the spectral image information and the original audio is obtained effectively. Due to the effective selection of optimal embedding location leads to improve the overall system robustness, transparency and capacity requirements. More ever, the security problems are overcome using the sequence of encryption process. Thus, hybrid and intelligent audio steganography process ensures the complexity for intermediate users while accessing the data. Then the efficiency of stem is evaluated using experimental and result analysis.

4. Results and discussions

This section examines the excellence of hybrid discrete wavelet transform and discrete cosine transform with genetic algorithm-based audio steganography process. The discussed above system implemented using MATLAB tool on windows 8.1 operating systems with 1.6Hz intel processor, 3GB RAM and 250 GB hard disk. During the analysis, system utilizes the Audio Steganographic Dataset for examines the excellence of the system. The dataset consists of 44.1 kHz sampling rate of 33038 stereo wav from audio clips. The collected audio clips having 10s durations that consists of MP3 and .wav of audio files utilized for MP3 Steganalysis process. The gathered audio files are processed by discrete wavelet transform that divide the audio signal into the sub signals using low and high pass filter. Then the secrete image messages are further examined using discrete cosine transform that get the spectral information. This information's encrypted according to the varying length of keys presented in the advanced standard encryption process. Finally, the encrypted messages are embedded in the audio file according to the genetic operators selected locations. This process ensures the overall audio quality, security and minimize the computation complexity while transmitting data from senders to receivers. The excellence of the system is evaluated using different metrics such as PSNR, structural similarity index (SSIM), minimum mean square error value and Jaccard.

4.1 Performance metrics

4.1.1. Peak signal to noise ratio (PSRN)

The peak signal to noise ratio (PSNR) metric is used to identify the noise level presented in the audio signal. The PSNR value is measured by decibel (db) which is computed by the noise level present in the audio file with respective error value. The PSNR value is estimated as follows.

$$PSNR = 10.\log 10\left(\frac{Max_i^2}{MSE}\right) \quad (5)$$

According to Eq. (5), the PSNR value is computed using maximum image pixel Max_i^2 and error value MSE during the audio steganography analysis.

4.1.2. Mean square error rate (MSE)

The MSE value is used to compute the deviation between the original and Stego audio file after embedding the secrete messages into the original audio file. If the computed MSE value is low, then the entire steganography process ensures high accuracy or high quality.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad (6)$$

In eqn (6), $I(i,j)$ is the original image pixel value and the modified pixel value is denoted as $K(i,j)$. m,n is the height and width of the images.

4.1.3. Structural similarity index (SSIM)

Structural similarity index (SSIM) measure used to identify the quality of the image and audio clips after performing the steganography process. The SSIM value is computed using eqn (7).

$$SSIM = \frac{(2\mu_x\mu_y+c1)(2\sigma_{xy}+c2)}{(\mu_x^2+\mu_y^2+c1)(\sigma_x^2+\sigma_y^2+c2)} \quad (7)$$

The two windows x and y of common size n*n based SSIM is computed from x windows average (μ), variance (σ) of x and y. c1 and c2 are random parameters that stabilize the week denominator.

4.1.4. Jaccard Similarity Index

Jaccard similarity Index metric is used to identify the similarity between the sample audio signal and the Stego audio signal. This metric computes data quality by using eqn (8).

$$J = \frac{M11}{M01+M10+M11} \quad (8)$$

In eqn (8), M11 denoted that the total number of attributes having the both image A and having value 1, M01 denoted that number of attributes A is having 0 and B is 1, M10 is A image having 1 and B is having 0 and M00 represented that both images having 0 values.

4.2. Performance analysis

The above discussed performance metrics used to examine the introduced audio steganography process. Not only the audio Steganalysis dataset, different audio files of varying file size and various secrete image varying size is utilized to examine the efficiency of the introduced system. The obtained system PSNR, SSIM and Jaccard values is shown in table 1.

Table 1. Performance analysis

Audio file	Audio file size (bytes)	Image message size (bytes)	PSNR	Jaccard	SSIM
Bird sound wave file	315,292 bytes	12,023 bytes	92.34	93.28	92.89
Drum and Bass wave	463,190 bytes	12,124 bytes	89.20	94.13	95.23
Express wave	312,289 bytes	120245 bytes	91.89	93.89	92.19
Funky wave	213489 bytes	12288	92.97	94.10	93.13
Philtered wave	228913 bytes	12391	93.19	94.29	91.28

The above table 1 illustrated that the hybrid DWT and DCT with genetic algorithm-based audio steganography process PSNR, Jaccard and SSIM value. During the analysis process, different audio files with varying size and different secret image with varying sizes are utilized to perform the audio steganography. The different size of secret messages embedded in the audio file, during this process the quality of the original audio file is same as the Stego file. According to the table 1, graphical illustration is depicted in figure 4.

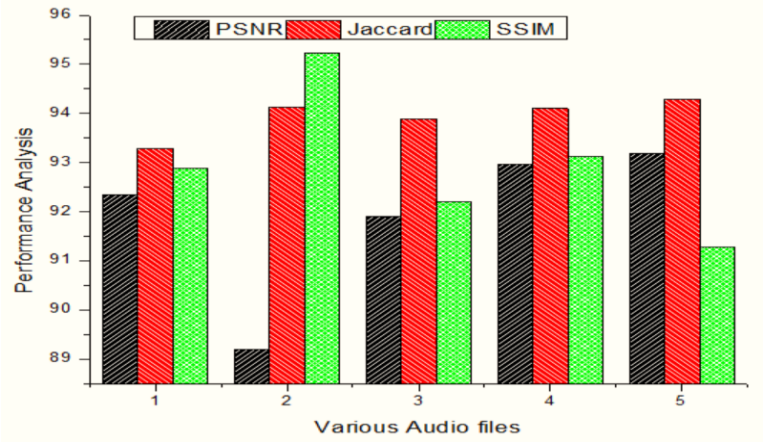

Figure 4. Performance Analysis of different audio files

From the figure 4 illustrated that the efficiency of the introduced audio steganography approach-based data security process. The introduced system examines the audio signal $\mathfrak{X}(n)$ and decompose the signal into approximation and detailed coefficients using $\sum_j \sum_k x(k) 2^{-j/2} \psi\left(2^{-j} n - k\right)$. Then, the secret images are further analyzed using cosine transform by applying the $\sum_{n_1=0}^{N_1-1} \left(\sum_{n_2=0}^{N_2-1} x_{n_1,n_2} \cos\left[\frac{\pi}{N_2}\left(n_2 + \frac{1}{2}\right) k_2\right]\right) \cos\left[\frac{\pi}{N_1}\left(n_1 + \frac{1}{2}\right) k_1\right]$. This process helps to examines the each and every pixels and frames in image and audio that increases the robustness of the steganography. Further, the security of the system is improved by encrypting the secret messages into different keys. This process maintains the capacity of the audio steganography. Although, this process improves the overall transparency and security of the data transmission. Further, the security is enhanced by embedding the secrete message in the optimal location that is done by genetic operators. The genetic operators select the new samples based on the chromosome fitness function. This optimized process enhances the overall efficiency of the system while utilizing different audio files in varying size and secret image with varying size. Further, the excellence of introduced method is compared to the existing approaches such as Haar discrete wavelet transform [27], deep residual networks [20] and genetically optimized 2D- discrete cosine transform [30]. The efficiency of the hybrid DWT and DCT with genetic algorithm (GA) approach excellency is evaluated on the Audio Steganographic Dataset with different size of secret image message. Then the obtained PSNR value of varying image message-based audio steganography process is illustrated in table 2.

Table 2. PSNR Analysis

Image size in Kb	50	100	150	200	250	300	350	400	450	500
[27]	73.7	78.37	75.37	76.27	77.29	78.29	76.28	76.73	78.29	79.28
[29]	78.28	82.38	76.29	78.28	82.38	81.23	79.38	82.38	79.29	83.18
[30]	82.38	84.28	86.38	79.38	84.76	86.28	86.39	86.20	84.78	86.29
Proposed	89.28	92.38	94.28	91.389	95.28	94.29	93.19	92.79	93.8	94.79

From the table 2 clearly demonstrated that the PSNR value of different researcher methodologies [27, 29, 30] and hybrid DWT with DCT and GA audio steganography analysis. The efficiency of PSNR values is compared with different size of secret image files. The high PSNR value indicates that introduced approach ensures the high security also without having any distortion while embedding the image into the audio file. The graphical illustration of PSNR value is shown in figure 5.

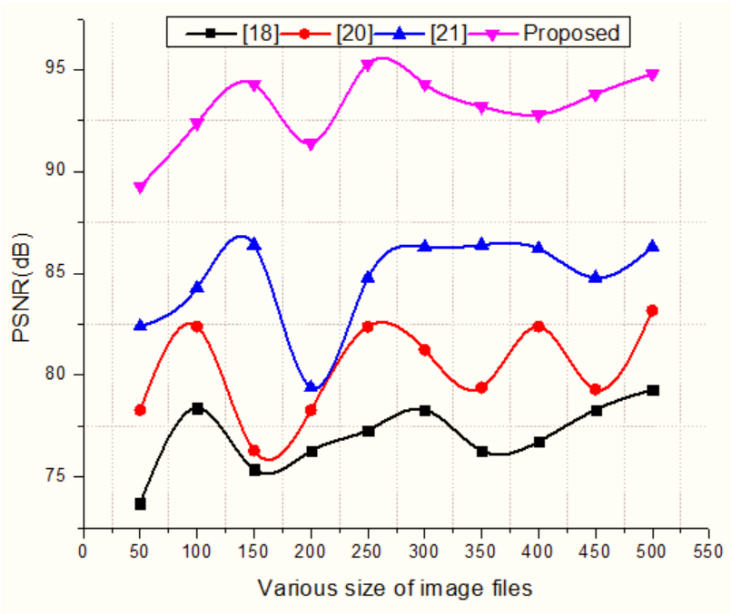

Figure 5. PSNR Analysis

The introduced DWT with DCT and GA approach successfully examine the audio signal using wavelet $y(n) = (\mathfrak{X} * g)n = \sum_{k=-\infty}^{\infty} \mathfrak{X}(k)g(n-k)$ process. The method utilizes the low and high pass filters for examining the audio approximation and detailed coefficients. These coefficients are more helpful to examines the audio signals and frame effectively. Then the extracted image file vectors are embedded according to the genetic operators such as selection, crossover and mutation. The optimal selection of embedding location varied according to the fitness function that improves the overall robustness of the audio steganography process. Due to the optimal selection of the secret message embedding location increases the overall efficiency of the system which is higher than compared to the other methods such as Haar discrete wavelet transform [27], deep residual networks [29] and genetically optimized 2D- discrete cosine transform [30]. The high PSNR value indicates that introduced method has maximum quality after performing the audio steganography. In addition to this, PSNR value, the SSIM of the original and Stego file should be analyzed and the obtained results are illustrated in figure 6.

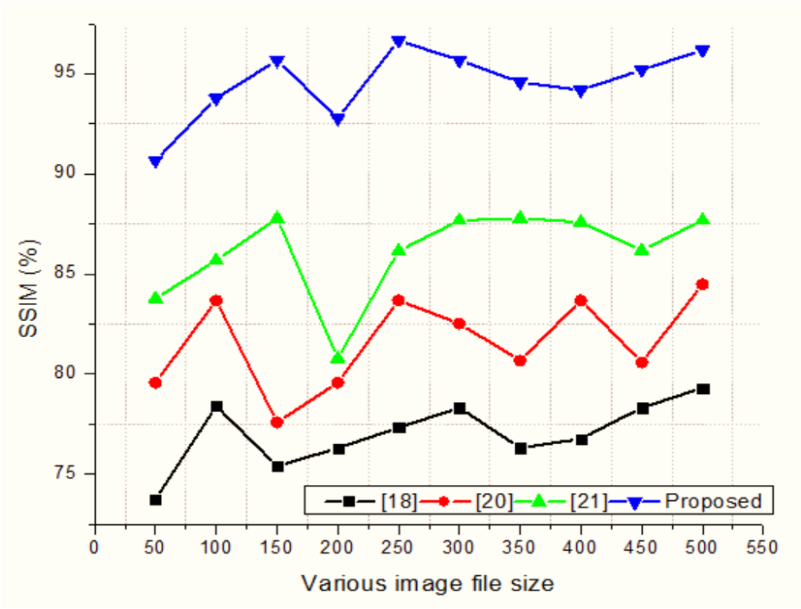

Figure 6. SSIM Analysis

From the figure 5 clearly demonstrated that the SSIM value of different researcher methodologies [27, 29, 30] and hybrid DWT with DCT and GA audio steganography analysis. The efficiency of SSIM values is compared with different size of secret image files. The high SSIM value indicates that introduced approach embedded

Stego files have same quality compared to the original audio file. The proposed method uses the alteration, modification, verification and reconstruction steps while embedding the secrete text files into the audio file. These steps use the selection, crossover and mutation operators for generating the new chromosomes or samples from the original audio samples. The selected optimal locations are used to embed the $\sum_{n_1=0}^{N_1-1}\left(\sum_{n_2=0}^{N_2-1} x_{n_1,n_2}\, cos\left[\frac{\pi}{N_2}\left(n_2+\frac{1}{2}\right)k_2\right]\right) cos\left[\frac{\pi}{N_1}\left(n_1+\frac{1}{2}\right)k_1\right]$ based extracted image secret vectors. The optimized selection embedding location improves the overall transparency, capacity, robustness and security. The efficiency of the system is evaluated using Jaccard Index value and the obtained results are illustrated in figure 7.

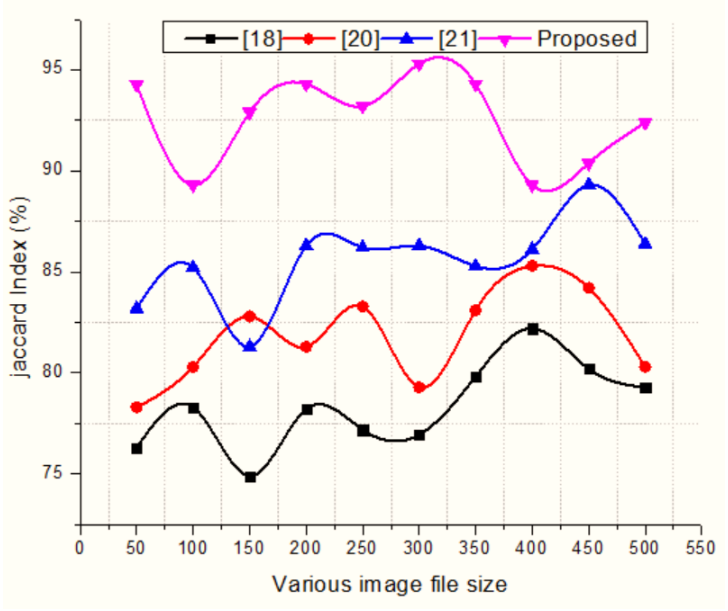

Figure 7. Jaccard Index Analysis

From the figure 6 clearly demonstrated that the Jaccard Index of different researcher methodologies [27, 29, 30] and hybrid DWT with DCT and GA audio steganography analysis. The efficiency of Jaccard index value is compared with different size of secret image files. The high Jaccard value indicates that introduced approach embedded Stego files are similar to the original audio files. Even though, the introduced method achieves high quality, the embedding process should have minimum error rate while doing the audio steganography. The obtained error rate illustrated in figure 8.

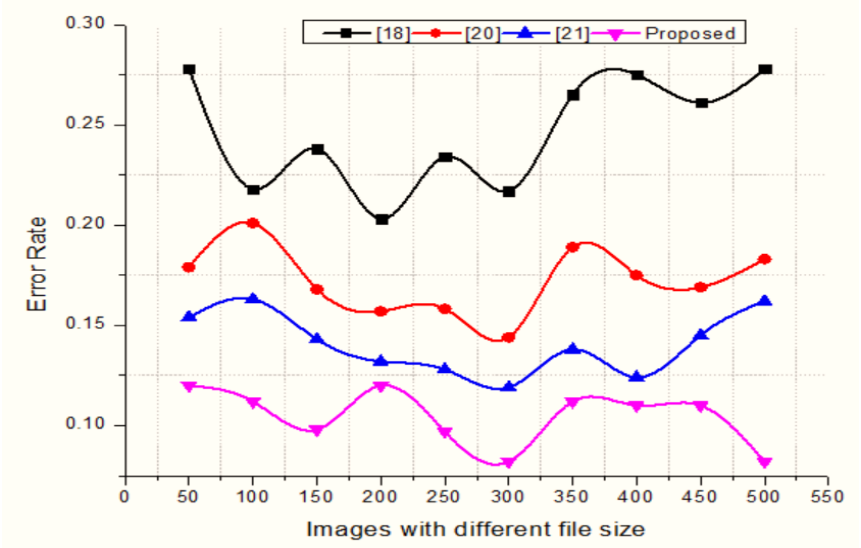

Figure 8. Error Rate

From the figure 7 clearly shows that hybrid DWT with DCT and GA approach attains the minimum error rate while embedding the image text file into the audio file. The minimum error value indicates that genetic operators such as selection, crossover and mutation operators selected locations are effective compared to other existing methods. Thus, the introduced hybrid DWT with DCT and GA algorithm ensures the system robustness, security, capacity and transparency while embedding the image files into the audio effectively.

5. Conclusion

Thus, the paper introduces the hybrid discrete wavelet transform with discrete cosine transform and genetic algorithm-based image embedding process in the audio file. This system uses the Audio Steganographic Dataset for analyzing the steganography process. The gathered audio files are processed by using wavelet transform that decompose the signals into sub-signals by examining the approximation and detailed coefficients. After that, the image based secret messages are computed using cosine transform that extracts the vectors. The extracted vectors are embedded into the audio signal by selecting the optimal image location which is selected according to the genetic operators. This process ensures the audio steganography characteristics such as robustness, capacity, transparency and security while transmitting data from sender to receiver. The introduced system ensures the minimum error rate (0.104), maximum SSIM (93.14%), PSNR (92.52%) and Jaccard Index (94.53%) value compared to other methods. In future, the efficiency of the system is improved using optimized embedding location process.

6. Reference

[1] J. O. Ejemeyovwi, E. S. Osabuohien, O. D. Johnson, and E. I. Bowale, "Internet usage, innovation and human development nexus in Africa: the case of ECOWAS," *Journal of Economic Structures,* vol. 8, no. 1, pp. 1-16, 2019.

[2] W.-C. Lu, "The impacts of information and communication technology, energy consumption, financial development, and economic growth on carbon dioxide emissions in 12 Asian countries," *Mitigation Adaptation Strategies for Global Change,* vol. 23, no. 8, pp. 1351-1365, 2018.

[3] I. Alsmadi, R. Burdwell, A. Aleroud, A. Wahbeh, M. Al-Qudah, and A. Al-Omari, "Introduction to information security," in *Practical Information Security*: Springer, 2018, pp. 1-16.

[4] P. Vörös, P. Hudoba, and A. Kiss, "Steganography and Cryptography for User Data in Calendars," in *Asian Conference on Intelligent Information and Database Systems*, 2019, pp. 241-252: Springer.

[5] S. S. L. Preeth, R. Dhanalakshmi, R. Kumar, and P. M. Shakeel, "An adaptive fuzzy rule based energy efficient clustering and immune-inspired routing protocol for WSN-assisted IoT system," *Journal of Ambient Intelligence Humanized Computing,* pp. 1-13, 2018.

[6] H. Alrikabi, and H. Tauma"Enhanced Data Security of Communication System using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 144-157, 2021.

[7] F. Djebbar, B. Ayad, K. A. Meraim, and H. Hamam, "Comparative study of digital audio steganography techniques," *EURASIP Journal on Audio, Speech, Music Processing,* vol. 2012, no. 1, pp. 1-16, 2012.

[8] A. G. M. Al-Dawoodi, "An improved Bees algorithm local search mechanism for numerical dataset," *Universiti Utara Malaysia,* 2015.

[9] N. A. H. Hala A. Naman, M. Al-dabag, H. Salim, "Encryption System for Hiding Information Based on Internet of Things," *International Journal of Interactive Mobile Technologies (iJIM),* vol. 15, no. 2, 2021.

[10] N. Al-Juaid and A. Gutub, "Combining RSA and audio steganography on personal computers for enhancing security," *SN Applied Sciences,* vol. 1, no. 8, pp. 1-11, 2019.

[11] P. F. Sheron, K. Sridhar, S. Baskar, and P. M. Shakeel, "A decentralized scalable security framework for end-to-end authentication of future IoT communication," *Transactions on Emerging Telecommunications Technologies,* vol. 31, no. 12, p. e3815, 2020.

[12] S. Zheng, L. Wang, B. Ling, and D. Hu, "Coverless information hiding based on robust image hashing," in *International conference on intelligent computing*, 2017, pp. 536-547: Springer.

[13] M. Mahmuddin and A. G. M. Al-dawoodi, "Experimental study of variation local search mechanism for bee algorithm feature selection," *Journal of Telecommunication, Electronic Computer Engineering,* vol. 9, no. 2-2, pp. 103-107, 2017.

[14] T. Srinivas and P. Amritha, "Real Time Audio Steganographic Countermeasure," in *Data Engineering and Intelligent Computing*: Springer, 2018, pp. 293-300.
[15] S. Baskar, P. M. Shakeel, R. Kumar, M. Burhanuddin, and R. Sampath, "A dynamic and interoperable communication framework for controlling the operations of wearable sensors in smart healthcare applications," *Computer Communications,* vol. 149, pp. 17-26, 2020.
[16] M. M. Aljamea, C. S. Iliopoulos, and M. Samiruzzaman, "Detection of url in image steganography," in *Proceedings of the International Conference on Internet of things and Cloud Computing*, 2016, pp. 1-6.
[17] K. Bansal, A. Agrawal, and N. Bansal, "A Survey on Steganography using Least Significant bit (LSB) Embedding Approach," in *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, 2020, pp. 64-69: IEEE.
[18] M. A. Al Mamun, S. M. Alam, M. S. Hossain, and M. Samiruzzaman, "A Novel Image Steganography Using Multiple LSB Substitution and Pixel Randomization Using Stern-Brocot Sequence," in *Future of Information and Communication Conference*, 2020, pp. 756-773: Springer.
[19] A. G. M. Al-dawoodi and M. Mahmuddin, "An empirical study of double-bridge search move on subset feature selection search of bees algorithm," *Journal of Telecommunication, Electronic Computer Engineering,* vol. 9, no. 2-2, pp. 11-15, 2017.
[20] I. A. Aljazaery, H. T. S. Alrikabi, and M. R. Aziz, "Combination of Hiding and Encryption for Data Security," *International Journal of Interactive Mobile Technologies,* vol. 14, no. 9, pp. 34-47, 2020.
[21] N. Sathisha, K. S. Babu, K. Raja, K. Venugopal, and L. M. Patnaik, "Covariance based steganography using DCT," in *International Conference on Advances in Computing and Communications*, 2011, pp. 636-647: Springer.
[22] S. Singh, R. Singh, and T. J. Siddiqui, "Singular value decomposition based image steganography using integer wavelet transform," in *Advances in signal processing and intelligent recognition systems*: Springer, 2016, pp. 593-601.
[23] H. TH, N. Alseelawi, and H. Tuama "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT " International Journal of Interactive Mobile Technologies (iJIM), 2021.
[24] C. Jin, R. Wang, and D. Yan, "Steganalysis of MP3Stego with low embedding-rate using Markov feature," *Multimedia Tools Applications,* vol. 76, no. 5, pp. 6143-6158, 2017.
[25] M. Chen, V. Sedighi, M. Boroumand, and J. Fridrich, "JPEG-phase-aware convolutional neural network for steganalysis of JPEG images," in *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, 2017, pp. 75-84.
[26] H. Salim, and N. A. Jasim, "Design and Implementation of Smart City Applications Based on the Internet of Things," *International Journal of Interactive Mobile Technologies (iJIM),* vol. 15, no. 13, pp. 4-15, 2021.
[27] Y. Taouil, E. B. Ameur, and M. T. Belghiti, "New image steganography method based on Haar discrete wavelet transform," in *Europe and MENA Cooperation Advances in Information and Communication Technologies*: Springer, 2017, pp. 287-297.
[28] R. Tanwar and S. Malhotra, "Opinion formation based optimization in audio steganography," in *International Conference on Information and Communication Technology for Intelligent Systems*, 2017, pp. 320-325: Springer.
[29] Z. Zhang, X. Yi, and X. Zhao, "Improving Audio Steganalysis Using Deep Residual Networks," in *International Workshop on Digital Watermarking*, 2019, pp. 57-70: Springer.
[30] R. Biswas and S. K. Bandyapadhay, "Random selection based GA optimization in 2D-DCT domain color image steganography," *Multimedia Tools Applications,* vol. 79, no. 11, pp. 7101-7120, 2020.
[31] S. M. Alwahbani and H. T. Elshoush, "Chaos-based audio steganography and cryptography using LSB method and one-time pad," in *Proceedings of sai intelligent systems conference*, 2016, pp. 755-768: Springer.
[32] A. Mohsin, A. Zaidan, B. Zaidan, O. Albahri, A. Albahri, M. Alsalem, K. Mohammed, S. Nidhal, N. S. Jalood, and A. N. Jasim, "New method of image steganography based on particle swarm optimization algorithm in spatial domain for high embedding capacity," *IEEE Access,* vol. 7, pp. 168994-169010, 2019.

[33] W. Luo, Y. Zhang, and H. Li, "Adaptive audio steganography based on advanced audio coding and syndrome-trellis coding," in *International Workshop on Digital Watermarking*, 2017, pp. 177-186: Springer.

[34] M. Dalal and M. Juneja, "Video steganography techniques in spatial domain—a survey," in *Proceedings of the international Conference on Computing and Communication Systems*, 2018, pp. 705-711: Springer.